Application for
UNITED STATES LETTERS PATENT

Of

MINORU OOGUSHI

For

VIRTUAL ACCESS ROUTER

W1319-01EU

仮想アクセスルータ

VIRTUAL ACCESS ROUTER

Background of the Invention

本発明は、アクセスルータおよびネットワークサーバの仮想機能に関する。

バックボーンネットワークまたはキャリアネットワークのエッジ部分で用いられる技術の一つに「仮想ルータ機能」がある。一般に、仮想ルータ機能とは、一台の装置をあたかも複数のルータのように扱うことのできる機能のことを言う。各仮想ルータは独立の経路情報を持ち、IPルーティングをはじめとする各種プロトコル（ARP、ICMP、RADIUS、SNMP等）は仮想ルータ（VR1、VR2、…）毎に独立に動作する。仮想ルータの概要については、2000年9月発行のIETF RFC2917 “A Core MPLS IP VPN Architecture” に開示されている。

特開2001-268125号公報には、イントラネットの端末集線用のサーバに仮想ルータ機能を持たせ、ユーザが任意のVPNを選択できるようにする技術が開示されている。

一方、近年、エンドユーザのインターネットアクセス環境は急速にブロードバンド化が進展している。ブロードバンドアクセスの実現には、ADSL、FTTH、CATV等の広帯域アクセス回線技術が用いられている。ブロードバンドアクセスを事業形態の観点から見ると、「プロバイダ一体型アクセス」と「プロバイダ選択型アクセス」の二つの形態が共存している。

「プロバイダ一体型アクセス」とは、単一の事業者がアクセス回線の提供からインターネット接続サービスまでトータルに行う事業形態である。一方「プロバイダ選択型アクセス」は、アクセス回線事業者がADSL、FTTH等のアクセス回線を提供し、インターネット接続サービスは複数のISP事業者が行うという分業型の事業形態である。歴史的な経緯や、ユーザ、ISPにとっての使い勝手の良さなどから、現時点では、プロバイダ選択型アクセスが主流になりつつある。

図１は、従来のプロバイダ選択型アクセスを実現するネットワークの一例を示す。図１の下部に示された図は、ネットワーク内に配置された各ネットワーク機器で使用されるプロトコルスタックを示す。アクセス回線としてはADSL、アクセスプロトコルにPPPoEの使用を想定している。

ユーザ宅内ではPC101がADSLモデム102に接続されている。ADSLモデム102は加入者電話回線に接続される。加入者電話回線は加入者収容局内にコロケーションされたアク

セス回線事業者の保有するDSLAM111に接続される。なお、加入者電話回線は本来電話サービスのための電話交換網の一部であり、アナログ電話通信やISDN通信と共用される。DSLAM111は、LAC112に接続され、更にL2TP転送網に接続される。LACとは、L2TP Access Concentrator の略で、L2TP転送網113のユーザ宅側のエッジに配置されるアクセスルータの一種である。L2TP転送網113は、物理的には通常のIPルータからなる通常のIPネットワークであるが、通信プロトコルとしてL2TPが使用されている。L2TPとは、IPネットワーク上でPPPフレームを伝送するためのトンネリングプロコトルであり、アクセス回線網上では、事実上標準的に使用されているプロトコルである。L2TPの始点となるアクセスルータがLACであり、L2TPの終点となるアクセスルータがLNSである。

L2TP転送網113のISP網側には、LNS（L2TP Network Server）と呼ばれるアクセスルータが配置される。LNSは、GWを介して各ISP網に接続され、ユーザは、各ISPによって、インターネット150へアクセス可能となる。

アクセス回線事業者は、L2TP転送網113を介して複数のISP事業者と相互接続する。LNSは、L2TP転送網113のエッジ部分に位置し、ISP事業者との相互接続点における、アクセス回線事業者側のゲートウェイルータの役割を果たす。複数のISP事業者と相互接続するために、ISP事業者毎に別々のLNSが必要とされる。また、L2TP転送網内に複数のL2TPトンネルを形成するためには、L2TPトンネルの数に対応した数のLACも必要となる。

Summary of the Invention

従来のプロバイダ選択型アクセスにおいては、LACないしLNSに関して以下のような課題があった。

１．LACにおける課題

従来のLAC装置は経路情報を複数保持することができず、複数の独立したIPネットワークと接続することが困難であった。そのため、L2TP転送網は通常のIPネットワークで良いにも拘わらず、従来はアクセス回線事業者が自前で広域ネットワークを構築していた。

２．LNSにおける課題

従来のLNS装置は、経路情報を複数保持することができず、複数の独立したIPネットワークと接続することが困難であった。各々のISPは、IPアドレス、経路情報、サービス品質等を自身のポリシーに基づいて制御する必要があるため、アクセス回線事業者は接続先となるISP毎に別々のLNS装置を用意する必要があり、その設置コストがアク

セス回線事業者の負担になっていた。

本発明は上記のような従来技術の問題を解消しうる仮想アクセスルータを提供することを目的とする。

上記目的を達成すべく、本発明の一面によれば、LACまたはLNSを構成するアクセスルータに仮想ルータ機能を持たせる。アクセスルータには、受信パケットの属性に対応して送受信用のインタフェースを持たせ、当該インタフェースを介して送受信されるパケットの転送処理を特定の仮想ルータに受け持たせる。

本発明の一例においては、インタフェースは、アクセスルータに備えられる通信Ｉ/Ｆのいくつかを特定の属性の受信パケットに割り当てても良いし、アクセスルータ内で、論理的に実現される論理インタフェースに特定の属性のパケットを割り当てることで、インタフェースを実現しても良い。また、仮想ルータとインタフェースとの対応付け、すなわちマッピングは必ずしも固定ではなく、管理コンソールなどのユーザインタフェースを介した管理コマンド入力により設定変更可能である。管理コマンドは、通信Ｉ/Ｆを介して、リモート入力させても良い。

本発明に拠れば、LAC機能との連携において、1台のアクセスルータを異なる事業者の運用する複数のL2TP転送網と接続できるようになる。L2TP転送網は単なるIPネットワークであるため事業者間の相互接続が容易であり、複数事業者の連携による広域アクセスネットワークを構築することができる。

また、LNS機能との連携において、1台のアクセスルータを複数のISP網と接続することができる。また、L2TP転送網側のIPアドレス空間とISP網側のIPアドレス空間およびルーティングドメインを独立に設計することができ、またL2TP転送網を所有する事業者とISP事業者との連携が容易となる。また、上記以外にも~~発明が解決しようとする課題~~に記載した各課題を解決する。

SUMMERY OF THE INVENTION

本発明の他の目的、特徴及び利点は添付図面に関する以下の本発明の実施例の記載から明らかになるであろう。

Brief Description of the Drawings

図１は、従来のプロバイダ選択型アクセスの実現形態の一例を示す図；

図２は、本発明を実現するアクセスルータの内部構成の一例を示す図；

図３は、第１実施例の第1のマッピング方式に関する実施形態の一例を示す図；

図４は、第１実施例のＬＡＣ装置が配置されるネットワークのトポロジーの一例を示す図；

図５A, ５Bは、第1実施例で使用される論理インタフェーステーブルおよび経路情報テーブルを示す図；

図６は、第1実施例のマッピング方式における接続シーケンスの一例を示す図；

図７は、第２実施例の第1のマッピング方式に関する実施形態の一例を示す図；

図８A, ８Bは、第２実施例で使用される論理インタフェーステーブルおよび経路情報テーブルを示す図；

図９は、第２実施例のマッピング方式における接続シーケンスの一例を示す図；

図１０は、第３実施例の第1のマッピング方式に関する実施形態の一例を示す図；

図１１A, １１Bは、第３実施例で使用される論理インタフェーステーブルおよび経路情報テーブルを示す図；

図１２は、第３実施例のマッピング方式における接続シーケンスの一例を示す図；

図１３は、第４実施例の第1のマッピング方式に関する実施形態の一例を示す図；

図１４A, １４Bは、第４実施例で使用される論理インタフェーステーブルおよび経路情報テーブルを示す図；

図１５は、第４実施例のマッピング方式における接続シーケンスの一例を示す図；

図１６は、第5実施例の第1のマッピング方式に関する実施形態の一例を示す図；

図１７A, １７Bは、第5実施例で使用される論理インタフェーステーブルおよび経路情報テーブルを示す図；

図１８は、第5実施例のマッピング方式における接続シーケンスの一例を示す図；

図１９は、第６実施例の第1のマッピング方式に関する実施形態の一例を示す図；

図２０A, ２０Bは、第６実施例で使用される論理インタフェーステーブルおよび経路情報テーブルを示す図；及び

図２１は、第６実施例のマッピング方式における接続シーケンスの一例を示す図。

Detailed Description of the Embodiments

前述のマッピング方式に関して、以下の6種類がある。

１）LAC型・固定マッピング方式；

LAC機能を有するアクセスルータにおける、物理インタフェース単位または固定論理インタフェース単位に仮想ルータと関連付ける方式である。

２）LAC型・L2TPマッピング方式；

LAC機能を有するアクセスルータにおける、L2TPトンネル単位に仮想ルータと関連付ける方式である。

３）LAC型・PPPマッピング方式；

LAC機能を有するアクセスルータにおける、PPPセッション単位に仮想ルータと関連付ける方式である。

４）LNS型・固定マッピング方式；

LNS機能を有するアクセスルータにおける、物理インタフェース単位または固定論理インタフェース単位に仮想ルータと関連付ける方式である。

５）LNS型・L2TPマッピング方式；

LNS機能を有するアクセスルータにおける、L2TPトンネル単位に仮想ルータと関連付ける方式である。

６）LNS型・PPPマッピング方式；

LNS機能を有するアクセスルータにおける、PPPセッション単位に仮想ルータと関連付ける方式である。

以下の実施例では、上記１）～６）の方式に沿って、説明を行なう。なお、以下の実施例においては、LAC機能とはL2TP転送網にL2TPトンネルを形成する機能、LNS機能とはLACの形成したL2TPトンネルを終端する機能、バックボーンネットワークとは、特定のアクセスルータから見て、よりコアのネットワークに近いネットワーク全部をさすものとする。例えば、図１のネットワークトポロジーで云えば、LACから見たバックボーンネットワークとはL2TP転送網を含めた後段側のネットワーク全体を指し、LNSから見たバックボーンネットワークとは、ISP網を含めた、コアネットワークに近い後段側ネットワーク全体を指す。また、管理用コンテキストとは、アクセスルータの種々の設定が可能な動作モードを意味するものとする。

（アクセスルータ構成例）

図２は、以下の実施例で説明するアクセスルータ500の１実現形式を示す。

物理I/F処理部520は、物理インタフェース511～514を終端する。PHY処理部521でア

ナログ信号の変復調やアナログ/デジタル変換を行う。MAC処理部522でEthernetやATM等の媒体アクセス制御を行う。論理I/F処理部530との間では、物理インタフェースの種別に依存しない、レイヤ2以上のパケットデータを送受する。

物理I/F処理部520は仮想ルータ機能を意識する必要がないため、カードモジュールとすることで容易に増設可能な構成とすることができる。物理I/F処理部520とSW部540を除く全ての機能部は、仮想ルータ毎に独立に動作する必要がある。仮想ルータ毎の動作を実現する方法は複数考えられ、例えば、仮想ルータの数だけ独立に動作するプロセッサを搭載する方法、プロセッサは共通であるが仮想ルータの数だけ独立にプロセスを動作させる方法、プロセッサもプロセスも共通であるが内部的な仮想ルータ識別子を用いて区別する方法、等がある。本構成例では仮想ルータ識別子を用いる方法について説明する。この場合、仮想ルータへのマッピングは、個々のパケット毎に仮想ルータ識別子でマーキングすることによって実現される。

ＳＷ部530は、物理I/F処理部520で受信したパケットを各機能ブロックへ転送する。

転送処理部540は、物理I/F処理部520で受信したパケットのマッピング処理と受信パケットに対する経路制御処理を行なう機能ユニットである。詳しくは、PPPセッションやL2TPトンネル等、物理インタフェースで受信したパケットの属性を識別し、対応する仮想ルータにマッピングを行なう処理と、受信パケットに対するIPルーティングを行なう。ハードウェア構成としては、論理I/Fテーブル545と経路情報テーブル546が格納されたテーブルメモリ542とＣＰＵ541を含む。ＣＰＵ541には、装置起動時に補助記憶部520に格納されたプログラムがロードされ、検索制御プロセス543やEncap/Decap制御プロセス544が実行される。検索制御プロセス543は、論理I/Fテーブル545と経路情報テーブル546の検索を行い、検索結果をEncap/Decap制御プロセス544に渡す。検索制御プロセス543は、検索順序も制御する。経路情報テーブル546の検索の際には、物理I/F識別子、論理I/F識別子をキーエントリとして、仮想ルータ識別子、プロトコル種別、その他オプション情報が検索される。Encap/Decap制御プロセス544は、 論理I/Fテーブル545の検索結果に基づき、パケットのカプセル化／デカプセル化を行う。論理I/Fテーブル545や経路情報テーブル546の内容については後段で詳述する。論理I/Fテーブル545や経路情報テーブル546は、非常にデータ量が大きいので、ASIC、並列プロセッサ、CAMメモリ等の専用ハードを用いて処理を高速化する。

装置管理部550はアクセスルータ500の装置全体に関わる制御を行う。各種アプリケーションプロセスもこのブロックで動作する。実行されるプロセスの例として、OSPFやBGP等のルーティングプロセス、SNMPエージェント等のマネジメントプロセス、

Telnetサーバ等のリモートログインプロセス、RADIUSクライアント等のAAAプロセス等が挙げられる。これらのプロセスは仮想ルータ毎に異なる設定で動作し、メッセージングを行う際の自宛IPアドレスや対向装置のIPアドレスも仮想ルータ毎に異なる。これらの設定情報や収集した統計情報等は、仮想ルータ識別子を用いて区別して管理される。

装置管理部550のハードウェア構成としては、メモリ552とＣＰＵ551からなり、装置起動時に、各種アプリケーションプロセスを実行するためのプログラムが補助記憶部560からＣＰＵ551にロードされる。仮想ルータ管理プロセス553は、仮想ルータの作成・削除、各仮想ルータにおけるマッピング設定、各種リソース設定・動作設定を制御する。これらの仮想ルータ構成情報は仮想ルータデータプロファイル554において管理される。運用設定がLAC型/LNS型のいずれであるか、マッピング設定が固定マッピング/L2TPマッピング/PPPマッピングのいずれであるかに応じて仮想ルータ間の連携や排他制御が管理される。

シーケンス制御プロセス556は、PPPやL2TPの接続シーケンスの制御を行う。仮想ルータ管理プロセス553や仮想ルータデータプロファイル554と連携することにより、各種の接続シーケンスを実行する。

コマンド処理プロセス555は、コンソールポートやTelnetログインのポートに対してシェル機能を提供し、各種コマンドを受け付ける。コマンド内容を解析し、対応する構成情報の変更を仮想ルータ管理プロセス553へ依頼する。例えばマッピング設定を追加/変更コマンドを実行した場合には、論理I/Fテーブル531の対応するエントリが追加/変更される。また、コマンド処理プロセス555は仮想ルータ識別子に対応するコンテキストを有し、各々のコンテキストにおける各コマンドの実行権限を管理する。

補助記憶部560は、プログラムプログラムコード561やデフォルト設定、ユーザ設定等のパラメータ群562を保存する。プログラムコード561は、ＣＰＵ551や541が実行する各種アプリケーションのことであり、装置起動時にメモリ542、552にロードされる。プログラムコード561の例として、OSPFやBGP等のルーティングプロセス、SNMPエージェント等のマネジメントプロセス、Telnetサーバ等のリモートログインプロセス、RADIUSクライアント等のAAAプロセス等が挙げられる。これらのプロセスは仮想ルータ毎に異なる設定で動作し、メッセージングを行う際の自宛IPアドレスや対向装置のIPアドレスも仮想ルータ毎に異なる。これらの設定情報や収集した統計情報等は、仮想ルータ識別子を用いて区別して管理される。本実施例では、補助記憶部としてフラッシュメモリを想定しているが、EPROM等他の記憶手段を用いても構わない。

【第1実施例】

図３は、本実施例の第1のマッピング方式（LAC型・固定マッピング方式）に関する実施形態の一例であり、アクセスルータおよびネットワークの構成を示す。また、図４には、本実施例のＬＡＣ装置が配置されるネットワークのトポロジー図を示す。なお、特に断らない限り、後段の実施例で示すＬＡＣ、ＬＮＳ装置は、図４に示すネットワークに配置されているものとする。

VR0（610）は、アクセスルータ500の装置全体に関わる管理権限を有する特別な仮想ルータであり、アクセス回線事業者が管理する。またVR0（610）に関連付けられたインタフェース620は、TelnetやSNMPでアクセスするための管理用のインタフェースとなる。管理者は例えば、インタフェース620を経由してTelnetを実行することにより、VR0（610）のコンテキストにログインし、VR1～3（611～613）を作成したり、アクセス回線用インタフェース621～623を各々VR1～3（611～613）に関連付ける設定を実行することができる。

アクセス回線用インタフェース621～623は、VR0（610）の管理権限によってVR1～3（611～613）の各々へ固定的に関連付けられた物理インタフェースまたは物理インタフェースに多重された固定論理インタフェースである。同様に、L2TP転送網用インタフェース631～633は、VR0（610）の管理権限によってVR1～3（611～613）の各々へ固定的に関連付けられた物理インタフェースまたは物理インタフェースに多重された固定論理インタフェースである。なお、物理インタフェースに多重された固定論理インタフェースの例としては、ATM PVC、IEEE802.1Q TAG VLAN、MPLSラベルパス、また、該物理インタフェース上で複数のプロトコルを多重化する場合の、各々のプロトコルに対応する設定単位であるサブインタフェース、等が挙げられる。

VR1～3（611～613）は、従来のLAC型アクセスルータをアクセスルータ500の単一筐体内に並列化したイメージに対応する。図３中、VR1～3（611～613）の下部に各々“V-LAC”（Virtual-LAC）と表記しているのは本イメージを意味したものである。アクセス回線用インタフェース621上で着信したPPPセッションは、VR1（611）へ固定的にマッピングされる。

同様に、アクセス回線用インタフェース622、623上で着信したPPPセッションは、各々VR2（612）、VR3（613）へ固定的にマッピングされる。また、これらのPPPセッションが多重されるL2TPはUDP/IP上のプロトコルであるが、その自IPアドレスや対向するLNSのIPアドレスはVR1～3（611～613）毎に全く独立に管理され、VR1～3（611～613）の各々の間でIPアドレスの空間が重複しても構わない。このことは、L2TP転送網651～653

が互いの存在を意識することなく全く独立に構築可能であることを意味する。L2TP転送網は単なるIPネットワークで良いので、アクセス回線事業ともISP事業とも異なる、従来存在しなかった「L2TPトンネルを中継する事業」が成立し得る。その際、アクセス回線事業者は単一のアクセスルータ500を用いて複数の中継事業者の網651～653と接続することが可能である。

VR1～3（611～613）は、自身に関連付けられたインタフェースに関わる管理権限を有するが、アクセスルータ500の装置全体に関わる管理権限は有さない。このことは、アクセス回線事業者がL2TP転送網651～653の各々を所有する事業者にVR1～3（611～613）を仮想的なLAC装置としてホールセール（卸売り、管理権限委譲）するのに適している。アクセス回線事業者はVR0（610）の管理権限、すなわちアクセスルータ500の装置全体の管理権限を有するので、L2TP転送網651～653を所有する事業者に管理権限を委譲したVR1～3（611～613）の運用状況を監視することができ、また必要に応じて権限委譲のレベルを設定したり、スーパバイザ権限により強制的なコマンド発行等も可能である。

VR1～3（611～613）は、各々のホールセール先となる中継事業者におけるエッジノードとしての役割を果たす。VR1～3（611～613）の各々でOSPF、BGP等のルーティングプロトコルを独立の設定で動作させることによって、L2TP転送網651～653の各々で独立にルーティングドメインを構築することができる。

従来、単一のLAC装置はISP毎に単一のL2TPトンネルを生成するだけであったが、LAC装置が本実施例に記載の仮想ルータ機能を備えることにより、ISP毎に加えてアクセス回線のサービス種別毎にも別々のトンネルを生成することができる。ここで、サービス種別とは、アクセス回線種別（ADSL、FTTH等）、アクセス回線帯域（1.5Mbps、8Mbps、12Mbps、24Mbps、40Mbps、100Mbps等）、QoSクラス（帯域保証、遅延保証等）等を意味する。図３では、同じISP1と契約したユーザであっても、1.5MbpsのADSLユーザであるか、8MbpsのADSLユーザであるか、100MbpsのFTTHユーザであるかに対応して、着信するアクセス回線用インタフェースが各々621、622、623となるように回線設計しているので、収容先の仮想ルータがVR1～VR3（611～613）に分岐し、結果的にそれぞれ異なるL2TPトンネル641、643、645に多重化される。L2TP転送網651、652、653は、それぞれ1.5MbpsのADSLサービス、8MbpsのADSLサービス、100MbpsのFTTHサービス専用に構築したIPネットワークであり、アクセス制御や帯域制御等、各々のサービスに適したネットワーク設計が可能である。このように、仮想ルータ機能を活用することによってユーザに提供するサービス種別毎に最適なネットワーク設計を行うことも可能となる。

ISP2、ISP3のサービスおよびユーザに関しても同様である。

各VR1～VR3（611～613）は、PPPセッションを多重化するL2TPトンネルを決定するのに、それぞれAAAサーバ661～663と連携する。AAAサーバは、認証処理やアカウンティング処理のトランザクションが集中するため、多数のユーザを収容するためには負荷分散機構の実現が必須であるが、本実施例に拠れば多数のユーザを複数の仮想ルータに分散させて収容することによって、負荷分散のための独自機能に頼ることなく自然な形でAAAサーバの負荷分散が実現される。勿論、VR1～3（611～613）に共通に接続するネットワークを用意すれば、単一のAAAサーバをVR1～VR3（611～613）で共用することも可能である。収容するユーザ数がそれほど多くない、中規模程度のアクセスネットワークを構築する際にはこのような構成も有用である。

図5Aおよび図5Bには、本実施例で用いられる論理Ｉ/Ｆテーブル545と経路情報テーブル546の内容を示す。論理Ｉ/Ｆテーブルは、仮想ルータ識別子を格納する仮想ルータフィールド2001、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2002、受信パケットのプロトコルの種別を示す識別子を格納するプロトコルフィールド2003、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2004、該当する物理Ｉ/Ｆおよび論理Ｉ/Ｆが、パケットの送信送信（transmit）を行なう通信Ｉ/Ｆか、パケットを着信（receive）する通信Ｉ/Ｆかの別を示す値が格納されるDirectionフィールド2005、当該パケットに対して実行するべき処理内容を示す情報が格納されるアクションフィールド2006および仮想ルータフィールド2007からなる。物理Ｉ/Ｆ識別子としては、例えば、ATM_11やEther_12等、受信パケットが属するセッションで使用されているプロトコルに適当な数字を加えた識別子や、あるいは単純にポート番号等を使用する。

経路情報テーブル546は、仮想ルータ識別子を格納する仮想ルータフィールド2011、受信パケットの宛先IPアドレスが格納される宛先IPアドレスフィールド2012、アドレスマスクが格納されるアドレスマスクフィールド2013、処理しようとするパケットが自宛パケットかそうでないかを示す識別子が格納される自宛フィールド2014、next hopノードのアドレスが格納されるNext Hopアドレスフィールド2015、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2016、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2017からなる。

図６は、本実施例における接続シーケンスの一例である。これらのシーケンスの実行制御は、図２に示したアクセスルータ構成例においてはシーケンス制御部573が行う。仮想ルータ管理部571や仮想ルータ構成テーブル572と連携することにより、運用設定がLAC型/LNS型のいずれであるか、マッピング設定が固定マッピング/L2TPマッピング

/PPPマッピングのいずれであるかを識別し、図６のシーケンスのいずれかを実行する。

以上、本実施例に記載のLACにより、以下のような効果が得られる。

１）１台のLAC装置で経路情報を複数保持することができるので、複数の独立したIPネットワークと接続することが容易となる。従って、L2TP転送網として、複数のアクセス回線事業者ないし複数の通信事業者が提供するIPネットワークを用いることが可能となる。これにより、色々な事業形態が可能となる。

２）LAC装置の管理権限を、LAC装置に実現される仮想ルータ毎にアクセス回線事業者／通信事業者に委譲することができるので、アクセス回線事業者が他の通信事業者に対して前記各種機能のいずれかまたは全ての機能をホールセール（卸売り、管理権限委譲）する等の事業形態の成立する余地が生まれる。

３）サービス種別毎に別々のLAC装置を接地する必要が無く、１台のLAC装置ですむ。従って、アクセス回線事業者に取ってのコストメリットが大きい。

４）仮想ルータ毎に別々のAAAサーバと連携することから、装置全体のセッション収容数が仮想ルータ毎に振り分けられる結果として、従来技術によりAAAサーバの負荷分散を実施したのと同等の効果が得られる。

【第２実施例】

図７は、本発明の第２のマッピング方式（LAC型・L2TPマッピング方式）に関する実施形態の一例であり、アクセスルータおよびネットワークの構成を示す。

VR0（710）は、第1実施例の場合と同様にアクセスルータ500の装置全体に関わる管理権限を有するが、第1実施例と異なる点として全てのアクセス回線用インタフェース721を管理する役割を担う。VR0（710）は通常のLAC装置と同様にユーザからのPPP接続要求を着信し、AAAサーバ730と連携してドメイン識別情報（例：“ispl.co.jp”）からL2TPトンネル751～753のいずれに多重化するかを決定する（手順(1)）。次にL2TPトンネル751～753はそれぞれVR1～3（711～713）へマッピングされ（手順(2)）、該トンネルは該仮想ルータによって管理される。該トンネルの自IPアドレスや対向するLNSのIPアドレスは該仮想ルータの経路情報として各々独立に管理される。一方、L2TP転送網用インタフェース741～743は、VR0（710）の管理権限によってVR1～3（711～713）の各々へ固定的に関連付けられた物理インタフェースまたは物理インタフェースに多重された固定論理インタフェースである。

L2TP転送網761～763は各々VR1～3（711～713）と接続されているので、互いの存在を意識することなく全く独立に構築可能である。このようにして、第1実施例の場合と同様の「L2TPトンネルを中継する事業」が成立し得る。その際、アクセス回線事業者

は単一のアクセスルータ500を用いて複数の中継事業者の網761～763と接続することが可能である。

VR0（710）はアクセス回線事業者の管理専用の仮想ルータであると同時に、全てのPPPセッションのL2TPトンネルへの多重化を管理しているという意味でLAC機能の主要部分を提供する言わば「代表VR」であり、従来のLAC型アクセスルータのイメージに対応する。図中、VR0（710）の下部に“V-LAC”（Virtual-LAC）と表記しているのは本イメージを意味したものである。

第1実施例の場合と異なり、AAAサーバ730はVR0（710）に接続され、全てのPPPセッションのL2TPトンネルへの多重化を管理する。なおAAAサーバ730はVR0（710）とIP通信可能であれば良く、必ずしも直接接続する必要はない。例えばアクセス回線事業者が管理専用のIPネットワークを構築し、管理用インタフェース720を経由してVR0（710）とAAAサーバ730がIP通信可能であれば良い。

VR1～3（711～713）は、対応する中継事業者1～3へホールセール（卸売り、管理権限委譲）し、その設定管理を委ねることが可能である。但し、第1実施例におけるホールセールの対象は「仮想的なLAC装置」であったのが、本実施例におけるホールセールの対象は「仮想的なルータ装置」であり、LAC装置としての基本設定の大部分はVR0（710）の管理対象であってVR1～3（711～713）の管理権限外である。例えばVR1（711）の管理権限外の設定情報としては、問い合わせ先のAAAサーバ730に関する設定、PPPセッションのL2TPプロトコルへの多重化方法に関する設定等がある。但しLAC装置に固有の設定であっても、VR0（710）がVR1（711）に対して特別に管理権限を付与する設定を行っている場合には、L2TPトンネル751のセットアップ情報を、AAAサーバ730から取得する情報を上書きする形で設定可能とすることもできる。VR2（712）、VR3（713）に関しても同様である。

VR1～3（711～713）は、各々のホールセール先の中継事業者におけるエッジノードとしての役割を果たす。VR1～3（711～713）の各々でOSPF、BGP等のルーティングプロトコルを独立の設定で動作させることによって、L2TP転送網761～763の各々で独立にルーティングドメインを構築することができる。

本マッピング方式ではL2TPトンネルの単位でマッピング先の仮想ルータが制御されるので、PPPセッションの多重化先となるL2TPトンネルを決定することがそのまま該PPPセッションの経由先となる仮想ルータを決定することにつながる。多重化先となるL2TPトンネルを決定する手順は従来のLAC装置における手順と同様であり前述のようにドメイン識別情報を用いるが、後述の第３実施例に示すのと同様に、ドメイン識別

情報にサービス識別情報を含めることにより、該PPPセッションが指定したサービス識別情報に対応して、経由先の仮想ルータおよびL2TP転送網を決定することが可能となる。

図8Aおよび図8Bには、本実施例で用いられる論理Ｉ/Ｆテーブル545と経路情報テーブル546の内容を示す。論理Ｉ/Ｆテーブルは、仮想ルータ識別子を格納する仮想ルータフィールド2101、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2102、受信パケットのプロトコルの種別を示す識別子を格納するプロトコルフィールド2103、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2104、該当する物理Ｉ/Ｆおよび論理Ｉ/Ｆが、パケットの送信送信（transmit）を行なう通信Ｉ/Ｆか、パケットを着信（receive）する通信Ｉ/Ｆかの別を示す値が格納されるDirectionフィールド2105、当該パケットに対して実行するべき処理内容を示す情報が格納されるアクションフィールド2106および仮想ルータフィールド2107からなる。物理Ｉ/Ｆ識別子としては、例えば、ATM_11やEther_12等、受信パケットが属するセッションで使用されているプロトコルに適当な数字を加えた識別子や、あるいは単純にポート番号等を使用する。

経路情報テーブル546は、仮想ルータ識別子を格納する仮想ルータフィールド2111、受信パケットの宛先IPアドレスが格納される宛先IPアドレスフィールド2112、アドレスマスクが格納されるアドレスマスクフィールド2113、処理しようとするパケットが自宛パケットかそうでないかを示す識別子が格納される自宛フィールド2114、next hopノードのアドレスが格納されるNext Hopアドレスフィールド2115、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2116、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2117からなる。

図９は、本実施例における接続シーケンスの一例である。これらのシーケンスの実行制御は、図２に示したアクセスルータ構成例においてはシーケンス制御部573が行う。仮想ルータ管理部571や仮想ルータ構成テーブル572と連携することにより、運用設定がLAC型/LNS型のいずれであるか、マッピング設定が固定マッピング/L2TPマッピング/PPPマッピングのいずれであるかを識別し、図９のシーケンスのいずれかを実行する。

以上、本実施例に記載のLACにより、以下のような効果が得られる。

１）１台のLAC装置で経路情報を複数保持することができるので、複数の独立したIPネットワークと接続することが容易となる。従って、L2TP転送網として、複数のアクセス回線事業者ないし複数の通信事業者が提供するIPネットワークを用いることが可能となる。これにより、色々な事業形態が可能となる。

２）LAC装置の管理権限を、LAC装置に実現される仮想ルータ毎にアクセス回線事業者

／通信事業者に委譲することができるので、アクセス回線事業者が他の通信事業者に対して前記各種機能のいずれかまたは全ての機能をホールセール（卸売り、管理権限委譲）する等の事業形態の成立する余地が生まれる。

３）サービス種別毎に別々のLAC装置を接地する必要が無く、１台のLAC装置ですむ。従って、アクセス回線事業者に取ってのコストメリットが大きい。

また、第1実施例では特定のユーザの仮想ルータへのマッピングは固定的であったのが、本実施例ではセッション確立時に動的にマッピングが決定されるため、同一のユーザであっても接続の度毎に異なる仮想ルータを経由させることによって異なるサービスを提供することが可能となる。

【第３実施例】

図１０は、本発明の第３のマッピング方式（LAC型・PPPマッピング方式）に関する実施形態の一例であり、アクセスルータおよびネットワークの構成を示す。

本実施例では、ユーザ情報文字列を構成するドメイン識別情報は“service-a.isp1.co.jp”のような構造を持つ。ここで“service-a”はサービス識別情報であり、“isp1.co.jp”はISP識別情報である。サービス識別情報は、許容最大帯域、QoSクラス等のような、何らかのサービス種別を表す。

VR0（810）は、第1実施例の場合と同様にアクセスルータ500の装置全体に関わる管理権限を有し、また第２実施例の場合と同様に全てのアクセス回線用インタフェース821を管理する役割を担う。VR0（810）は通常のLAC装置と同様にユーザからのPPP接続要求を着信した後、ISP識別情報（例：“isp1.co.jp”）に基づき該PPP接続要求をVR1～3（811～813）のいずれにマッピングするかを決定する（手順(1)）。すなわち、ISP1への契約ユーザのPPP接続要求は全てVR1（811）へ振り分けられる。VR1（811）は、あたかも通常のLAC装置であるかのように前記PPP接続要求を着信し、AAAサーバ861と連携し、サービス識別情報（例：“service-a”）に基づく等して多重先のL2TPトンネル841を決定する（手順(2)）。VR2（812）、VR3（813）に関しても同様である。このようにして、ISP毎に別々にL2TP転送網851～853を構築し、さらに各々のISPにおけるサービス種別毎にL2TPトンネル841～846を構成することが可能である。

VR0（810）はアクセス回線事業者の管理専用の仮想ルータであると同時に、アクセス回線用インタフェース821を一括して管理し、またPPPセッションのVR1～3（811～813）へのマッピングを管理するという意味で言わば「代表VR」であるが、AAAサーバ861～863との連携やPPPセッションのL2TPトンネル841～846への多重化等のLAC機能を提供するのは、PPPセッションのマッピング先であるVR1～3（811～813）である。すな

わちVR1～3（811～813）は従来のLAC型アクセスルータのイメージに対応する。図中、VR1～3（811～813）の左下部分に“V-LAC”（Virtual-LAC）と表記しているのは本イメージを意味したものである。

L2TP転送網用インタフェース831～833は、VR0（810）の管理権限によってVR1～3（811～813）の各々へ固定的に関連付けられた物理インタフェースまたは物理インタフェースに多重された固定論理インタフェースである。

VR1～3（811～813）は、対応するISP1～3へホールセール（卸売り、管理権限委譲）し、その設定管理を委ねることが可能である。ホールセールの対象は第1実施例の場合と同様「仮想的なLAC装置」であるが、必要に応じてVR0（810）のスーパバイザ権限によりVR1～3（811～813）におけるL2TP機能の管理権限を制限しても良い。本実施例では、L2TP転送網851～853はISP1～3の各々が保有するIPネットワークである場合を想定しており、VR1～3（811～813）は各々あたかもISP1～3のエッジノードであるかのように運用することができる。VR1～3（811～813）の各々でOSPF、BGP等のルーティングプロトコルを独立の設定で動作させることによって、L2TP転送網851～853の各々で独立にルーティングドメインを構築することができる。またVR1～3（811～813）の各々が連携するAAAサーバ861～863は、各々L2TP転送網851～853内に設置される。このように本実施例では、アクセス回線事業者ではなく各々のISPが、仮想的なLAC装置、L2TP転送網、AAAサーバの各々を自身で管理する事業形態が可能である。

なお、VR1～3（811～813）毎に異なるAAAサーバ861～863と連携するので、第1実施例の場合と同様に、自然な形でAAAサーバの負荷分散が実現される。

本実施例においては、VR0（810）におけるPPPセッションのVR1～3（811～813）へのマッピング（手順①）を、ユーザ情報文字列に埋め込まれたサブ情報文字列に基づき行う例を示した。前記マッピングを行うために基づく情報としては、これ以外にも、PPPセッション単位で異なる値を持ち得る任意の属性情報であって構わない。そのような属性情報の例として、PPPoEセッションが確立する際にPC等ユーザ端末がPADRメッセージにより通知するService-Nameの値、LCPフェーズにおけるネゴシエーション結果の各種パラメータ値、PPP接続要求を着信した時点におけるVR1～3（811～813）のリソース占有情報、AAAサーバ861～863あるいは他のネットワーク監視サーバから取得したL2TP転送網851～853各々の輻輳情報、等が挙げられる。

図11Aおよび図11Bには、本実施例で用いられる論理Ｉ/Ｆテーブル545と経路情報テーブル546の内容を示す。論理Ｉ/Ｆテーブルは、仮想ルータ識別子を格納する仮想ルータフィールド2201、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2202、受信パ

ケットのプロトコルの種別を示す識別子を格納するプロトコルフィールド2203、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2204、該当する物理Ｉ/Ｆおよび論理Ｉ/Ｆが、パケットの送信送信(transmit)を行なう通信Ｉ/Ｆか、パケットを着信(receive)する通信Ｉ/Ｆかの別を示す値が格納されるDirectionフィールド2205、当該パケットに対して実行するべき処理内容を示す情報が格納されるアクションフィールド2206および仮想ルータフィールド2207からなる。物理Ｉ/Ｆ識別子としては、例えば、ATM_11やEther_12等、受信パケットが属するセッションで使用されているプロトコルに適当な数字を加えた識別子や、あるいは単純にポート番号等を使用する。

経路情報テーブル546は、仮想ルータ識別子を格納する仮想ルータフィールド2211、受信パケットの宛先IPアドレスが格納される宛先IPアドレスフィールド2212、アドレスマスクが格納されるアドレスマスクフィールド2213、処理しようとするパケットが自宛パケットかそうでないかを示す識別子が格納される自宛フィールド2214、next hopノードのアドレスが格納されるNext Hopアドレスフィールド2215、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2216、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2217からなる。

図１２は、本実施例における接続シーケンスの一例である。これらのシーケンスの実行制御は、図２に示したアクセスルータ構成例においてはシーケンス制御部573が行う。仮想ルータ管理部571や仮想ルータ構成テーブル572と連携することにより、運用設定がLAC型/LNS型のいずれであるか、マッピング設定が固定マッピング/L2TPマッピング/PPPマッピングのいずれであるかを識別し、図１２のシーケンスのいずれかを実行する。

以上のように、本実施例に記載のLACにより、第1実施例に記載した４つの効果の他、次のような効果が得られる。

第1実施例では特定のユーザの仮想ルータへのマッピングは固定的であったのが、本実施例ではセッション確立時に動的にマッピングが決定されるため、同一のユーザであっても接続の度毎に異なる仮想ルータを経由させることによって異なるサービスを提供することが可能となる。

また、広域のIPネットワークを有するISP事業者が、該IPネットワークを本実施例に記載のLACに直接接続することによって、L2TP転送網として使用することができる。

【第４実施例】

図１３は、本発明の第４のマッピング方式（LNS型・固定マッピング方式）に関する実施形態の一例であり、アクセスルータおよびネットワークの構成を示す。

VR0（910）は、アクセスルータ500の装置全体に関わる管理権限を有する特別な仮想ルータであり、アクセス回線事業者またはL2TP転送網930を所有する事業者が管理する。VR0（910）に関連付けられたインタフェース920は、第1実施例と同様、TelnetやSNMPでアクセスするための管理用のインタフェースである。例えば、管理者がインタフェース920を経由してTelnetを実行することにより、VR0（910）のコンテキストにログインし、VR1～3（911～913）を作成したり、L2TP転送網用インタフェース921～923を各々VR1～3（911～913）に関連付ける設定を実行することができる。

VR1～3（911～913）は、従来のLNS型アクセスルータをアクセスルータ500の単一筐体内に並列化したイメージに対応する。図１３中、VR1～3（911～913）の右下部分に各々“V-LNS”（Virtual-LNS）と表記しているのは本イメージを意味したものである。L2TP転送網用インタフェース921上で着信したL2TPトンネル931およびこれに多重されたL2TPセッションは、VR1（911）へ固定的にマッピングされる。同様に、L2TP転送網用インタフェース922、923上で着信したL2TPトンネル932、933およびこれらに多重されたL2TPセッションは、各々VR2（912）、VR3（913）へ固定的にマッピングされる。

図14Aおよび図14Bには、本実施例で用いられる論理Ｉ/Ｆテーブル545と経路情報テーブル546の内容を示す。論理Ｉ/Ｆテーブルは、仮想ルータ識別子を格納する仮想ルータフィールド2301、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2302、受信パケットのプロトコルの種別を示す識別子を格納するプロトコルフィールド2303、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2304、該当する物理Ｉ/Ｆおよび論理Ｉ/Ｆが、パケットの送信送信（transmit）を行なう通信Ｉ/Ｆか、パケットを着信（receive）する通信Ｉ/Ｆかの別を示す値が格納されるDirectionフィールド2305、当該パケットに対して実行するべき処理内容を示す情報が格納されるアクションフィールド2306および仮想ルータフィールド2307からなる。物理Ｉ/Ｆ識別子としては、例えば、ATM_11やEther_12等、受信パケットが属するセッションで使用されているプロトコルに適当な数字を加えた識別子や、あるいは単純にポート番号等を使用する。

経路情報テーブル546は、仮想ルータ識別子を格納する仮想ルータフィールド2311、受信パケットの宛先IPアドレスが格納される宛先IPアドレスフィールド2312、アドレスマスクが格納されるアドレスマスクフィールド2313、処理しようとするパケットが自宛パケットかそうでないかを示す識別子が格納される自宛フィールド2314、nexthopノードのアドレスが格納されるNextHopアドレスフィールド2315、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2316、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2317からなる。

以下に、図14Aおよび図14Bによるマッピング方法について説明する。図14Aおよび図14Bにおいては、仮想ルータ識別子は全てVR_1なので、従来のLNS装置と同等の動作となる。パケットの受信時には、2321～2328の順番でエントリが検索される。2321行の検索時には、Ether_21からIPパケットを受信、検索制御プロセス543が論理I/Fテーブル545を検索してエントリ2321にマッチ。アクション"Route"により、IPルーティングへ。2322行の検索時には、受信IPパケットの宛先IPアドレスが192.168.20.1。経路情報テーブル546を検索し、エントリ2322にマッチ、自宛（L2TPインタフェース）と知る。UDPの宛先ポート1701（L2TPの受信ポート）を得る。2323行の検索時には、論理I/Fテーブル545に戻り、UDPポート1701で検索してエントリ2323にマッチ。Encap/Decap制御プロセス544がUDP/IPヘッダをデカプセル化する。2324行の検索時には、L2TPヘッダのトンネルIDをキーに再び論理I/Fテーブル545を検索して、エントリ2324にマッチ。Encap/Decap制御プロセス544がL2TPヘッダをデカプセル化する。2325行の検索時には、L2TPヘッダのセッションIDをキーに再び論理I/Fテーブル545を検索して、エントリ2325にマッチ。Encap/Decap制御プロセス544がPPPヘッダをデカプセル化する。2326行の検索時には、ユーザデータであるIPパケットが取り出され、IPルーティングへ。2327行の検索時には、前記IPパケットの宛先IPアドレスが158.214.2.5（ユーザの通信先）。経路情報テーブル546を検索し、エントリ2327にマッチ、出力先の物理I/FがEther_22と知る。2328行の検索時には、論理I/Fテーブル545を検索してエントリ2328にマッチ。アクション"Forward"により、該IPパケットを物理I/F処理部520へ転送、Ether_22からの送信を指示。

パケットの送信時時には、2331～2338行の順番でエントリが検索される。上り方向とちょうど逆の処理手順を踏む。

VR1～3（911～913）をISP1～3の網（961～963）側に接続するインタフェース941～943は、VR0（910）の管理権限によってVR1～3（911～913）の各々へ固定的に関連付けられた物理インタフェースまたは固定論理インタフェースである。PC等ユーザ端末が送受信する、ユーザデータを構成するIPパケットは、PC等ユーザ端末からアクセスルータ500までの間はPPPにカプセル化されて送受信されるが、L2TPレイヤおよびPPPレイヤはVR1～3において終端されるので、インタフェース941～943上ではピュア・IPパケットとして送受信される。

VR1～3（911～913）の各々はあたかも独立のLNS装置であるかのように動作する。例えばVR1（911）は、L2TPトンネル931確立時に使用するLNSのホスト名、トンネルを終端するIPアドレス、連携するAAAサーバ971の情報、PC等ユーザ端末へ割り当てるIPア

ドレス情報、経路制御情報、サービス品質制御情報等を、VR2（912）、VR3（913）の存在を意識することなく独立に設定することができる。このように、VR1～3（911～913）を、それぞれISP1～3と接続するための独立した仮想LNS装置として運用することにより、アクセスルータ500の単一の物理筐体によって複数のISPとの接続が可能となるので、アクセス回線事業者またはL2TP転送網930を所有する事業者は、L2TP転送網930に接続するISPの数だけのLNS装置を設置する必要がない。ISP1～3の網（961～963）は互いにネットワーク的に分離しており、ルーティング情報の独立性が保たれる。各ISPは互いの存在を意識することなく、自由なルーティング設定が可能である。ISP1～3の各々が全く同一のプライベートIPアドレスの空間を使用する場合も、互いの存在が意識されないので、それぞれが該アドレス空間を独立に占有することができる。このような各種ネットワークリソースの高度な独立性は、従来技術に基づくLNS装置では実現不可能であり、そのため単一の物理筐体によって複数のISPとの接続を処理する運用が行われることもなかった。

VR1～3（911～913）は、自身に関連付けられたインタフェースに関わる管理権限を有するが、アクセスルータ500の装置全体に関わる管理権限は有さない。このことは、アクセス回線事業者またはL2TP転送網930を所有する事業者がISP事業者1～3にVR1～3（911～913）の各々を仮想的なLNS装置としてホールセール（卸売り、管理権限委譲）するのに適している。アクセス回線事業者またはL2TP転送網930を所有する事業者はVR0（910）の管理権限、すなわちアクセスルータ500の装置全体の管理権限を有するので、ISP事業者1～3に管理権限を委譲したVR1～3（911～913）の運用状況を監視することができ、また必要に応じて権限委譲のレベルを設定したり、スーパバイザ権限により強制的なコマンド発行等も可能である。

GW951～953は、図３に示したGW141と同等の役割を果たすものであり、例えばユーザからの不正アクセスを防止するために送信元IPアドレスが実際に割り当て中のアドレス以外であるようなIPパケットをブロックしたり、経路制御を自動化するためにOSPFやBGPといったルーティングプロトコルを動作させるのに必要である。

本実施例では、例えばVR1（911）はL2TP転送網930側とISP1網961側の両方に接続されている。このことは、L2TP転送網930とISP1網961がIPアドレスの空間を共有することを意味する。L2TP転送網930やISP1網961は閉域網であるため、各々プライベートIPアドレスを使用する場合があるが、L2TP転送網930とISP1網961の両方がプライベートIPアドレスを使用する場合、VR1（911）およびGW951のIPアドレス設定や経路制御設定において、互いの網のIPアドレス設計を意識した設定が必要となる。VR2（912）およ

びGW952、VR3（913）およびGW953に関しても同様であり、またこれらは図１に示した従来技術を用いた場合と同様である。

なお、ISP1へ接続するPC等ユーザ端末に割り当てられるIPアドレスは、VR1（911）がIPCPにより割り当てを行うが、IPアドレスの空間としてはISP1網961が管理する空間から割り当てられる。すなわちPC等ユーザ端末は論理的にはISP1網961に直収されたエンドノードである。そのため、ISP1網961がプライベートIPアドレスを使用する場合、PC等ユーザ端末にもプライベートIPアドレスが割り当てられる。一方、インターネット150への通信にはグローバルIPアドレスが必要である。このような場合、GW981において、PC等ユーザ端末のプライベートIPアドレスをインターネット150と通信可能なグローバルIPアドレスへ変換するためのNAT機能が必要である。GW982、GW983に関しても同様である。

前述のように、PC等ユーザ端末はISP1網961へ直収されているものとして扱われる。これは、通常の運用においてはPC等ユーザ端末からはL2TP転送網930の存在は隠蔽され、PC等ユーザ端末とL2TP転送網930内のノード等との間のIP通信は許容されないことを意味する。すなわち、VR1（911）はPC等ユーザ端末から送信されたIPパケットを、PPPおよびL2TPでカプセル化されたフォーマットで受信し、前記L2TPおよびPPPをデカプセル化して元のIPパケットを抽出するが、前記IPパケットの宛先IPアドレスが如何なる値であったとしてもGW951へ固定的にルーティングする必要がある。そのために、VR1（911）において、PC等ユーザ端末との間で確立したPPPセッション上で受信したIPパケットをGW951へ強制的にルーティングするためのポリシールーティングの設定を行うことが可能である。VR2（912）、VR3（913）に関しても同様であり、またこれらは図１に示した従来技術を用いた場合と同様である。

前述のように、VR1（911）はPC等ユーザ端末との間でのIPパケットの送受信をPPPおよびL2TPでカプセル化されたフォーマットで行うが、通常のIPルータと同様、L2TP転送網930とISP1網961との間で、PPPおよびL2TPでカプセル化されない（ピュア・IPの）フォーマットのIPパケットのルーティングも許容される。しかし、L2TP転送網930を管理するのはISP1とは別のアクセス回線事業者または中継事業者であるので、セキュリティの観点からピュア・IPパケットのルーティングを許容したくない場合もある。その場合には、VR1（911）において、ピュア・IPパケットのルーティングを抑止するためのパケットフィルタリングの設定を行うことが可能である。VR2（912）、VR3（913）に関しても同様であり、またこれらは図１に示した従来技術を用いた場合と同様である。

図１５は、本実施例における接続シーケンスの一例である。これらのシーケンスの実行制御は、図２に示したアクセスルータ構成例においてはシーケンス制御部573が行う。仮想ルータ管理部571や仮想ルータ構成テーブル572と連携することにより、運用設定がLAC型/LNS型のいずれであるか、マッピング設定が固定マッピング/L2TPマッピング/PPPマッピングのいずれであるかを識別し、図１５のシーケンスのいずれかを実行する。

以上、本実施例に記載のLACにより、以下のような効果が得られる。

１）従来と異なり、複数の経路情報を１台のLNSに収容できるので、複数の独立したIPネットワークと接続することが容易に実現できる。特に、IPアドレス体系、経路情報、サービス品質等に関するポリシーの異なる別々のISPであっても、１台のLNSを接続できる。

２）L2TP転送網のIPアドレス空間とISP網のIPアドレス空間を独立に設定管理することができるので、アクセス網からISP網までを含むネットワーク設計上の制約が低減される。

３）L2TP転送網とISP網の間のアクセス制御のために複雑なポリシールーティングやパケットフィルタリングの設定が必要無くなるので、運用管理コストを低減することができる。また、仮想ルータをISP毎に対応づけられるので、セキュリティドメインの完全な切り分けが実現される。

４）アクセス回線事業者とISP事業者のルーティングドメインの切り分けが可能となるため、め、ISP事業者側で、LNS装置と直接接続するためのゲートウェイ装置を用意する必要が無くなる。

５）LNS装置の管理権限を、LNS装置に実現される仮想ルータ毎にアクセス回線事業者／通信事業者に委譲することができるので、アクセス回線事業者が他の通信事業者に対して前記各種機能のいずれかまたは全ての機能をホールセール（卸売り、管理権限委譲）する等の事業形態の成立する余地が生まれる。

【第５実施例】

図１６は、本発明の第５のマッピング方式（LNS型・L2TPマッピング方式）に関する実施形態の一例であり、アクセスルータおよびネットワークの構成を示す。

VR0（1010）は、第４実施例の場合と同様にアクセスルータ500の装置全体に関わる管理権限を有し、またL2TP転送網用インタフェース1021～1023を管理する役割を担う。L2TPトンネル1024～1026およびそれらに多重されたL2TPセッションは、L2TP転送網用インタフェース1021～1023のいずれかを用いて受信される。L2TPトンネル1024～1026

およびそれらに多重されたL2TPセッションを構成するパケットはUDP/IPパケットであるが、VR0（1010）においてIPレイヤおよびUDPレイヤが終端される。VR0（1010）はL2TPトンネル1024～1026の各々に対応する内部的な論理インタフェースを持つが、これらはVR1～3（1011～1013）へ固定的にマッピングされている。結果的に、L2TPトンネル1024～1026は各々VR1～3（1011～1013）へマッピングされ、該マッピング先の仮想ルータにおいてL2TPレイヤが終端される。

図17Aおよび図17Bには、本実施例で用いられる論理Ｉ/Ｆテーブル545と経路情報テーブル546の内容を示す。論理Ｉ/Ｆテーブルは、仮想ルータ識別子を格納する仮想ルータフィールド2401、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2402、受信パケットのプロトコルの種別を示す識別子を格納するプロトコルフィールド2403、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2404、該当する物理Ｉ/Ｆおよび論理Ｉ/Ｆが、パケットの送信送信（transmit）を行なう通信Ｉ/Ｆかパケットを着信（receive）する通信Ｉ/Ｆかの別を示す値が格納されるDirectionフィールド2405、当該パケットに対して実行するべき処理内容を示す情報が格納されるアクションフィールド2406および仮想ルータフィールド2407からなる。物理Ｉ/Ｆ識別子としては、例えば、ATM_11やEther_12等、受信パケットが属するセッションで使用されているプロトコルに適当な数字を加えた識別子や、あるいは単純にポート番号等を使用する。

経路情報テーブル546は、仮想ルータ識別子を格納する仮想ルータフィールド2411、受信パケットの宛先IPアドレスが格納される宛先IPアドレスフィールド2412、アドレスマスクが格納されるアドレスマスクフィールド2413、処理しようとするパケットが自宛パケットかそうでないかを示す識別子が格納される自宛フィールド2414、nexthopノードのアドレスが格納されるNextHopアドレスフィールド2415、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2416、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2417からなる。

以下に、図17Aに示す論理Ｉ/Ｆテーブルおよび図17Bに示す経路情報テーブルを用いたマッピング方法について説明する。

各フィールドに格納される値は、仮想ルータ識別子フィールド以外は、第４実施例に示した値と同じ値が格納されている。上り方向の検索時には、2421～2428行の順番でエントリが検索される。2423行の検索時には、L2TPパケット（＝IPパケット）の受信はVR_0で行われ、IPおよびUDPを終端（デカプセル化）した後に、VR_1へマッピングされる。2424～行の検索時には、VR_1でL2TPおよびPPPが終端（デカプセル化）され、ユーザのIPパケットはVR_1の経路情報に基づきISP網へルーティングされる。下り方向

行の検索時には、2431～2438の順番でエントリが検索される。2434行の検索時には、PC等ユーザ端末宛のIPパケットはVR_1で受信され、PPPおよびL2TPにカプセル化された後にVR_0へマッピングされる。2435～行の検索時には、L2TPパケット（＝IPパケット）はVR_0の経路情報に基づきLAC装置宛にルーティングされる。

VR0（1010）はアクセス回線事業者またはL2TP転送網1030を所有する事業者の管理専用の仮想ルータであると同時に、L2TP転送網用インタフェース1021～1023を一括して管理し、全てのL2TPパケットのIPレイヤおよびUDPレイヤを終端し、L2TPトンネルのVR1～3（1011～1013）へのマッピングを管理するという意味で言わば「代表VR」である。一方、L2TPトンネルのマッピング先であるVR1～3（1011～1013）は、AAAサーバ1061～1063と連携してユーザ認証を行い、PC等ユーザ端末との間でPPPセッションを確立するという意味で従来のLNS型アクセスルータのイメージに対応する。図中、VR1～3（1011～1013）の右下部分に“V-LNS”（Virtual-LNS）と表記しているのは本イメージを意味したものである。

なお本実施例では、インタフェース1020は第４実施例におけるインタフェース920と同様の管理専用インタフェースと想定しているが、リモートログインを実現するためにL2TP転送網1030に接続するのであれば、必ずしも管理専用としなくても良い。インタフェース1021～1023と同様に、L2TPパケットの送受信にも同時に用いることも可能である。セキュリティ等への考慮から、特定のインタフェースに限定してリモートログインを許容したい場合等には、本実施例のように管理専用のインタフェースとL2TPパケットの送受信用のインタフェースを分けるのが良い。

VR1～3（1011～1013）とISP1～3の網（1051～1053）とを接続するインタフェース1041～1043は、VR0（1010）の管理権限によってVR1～3（1011～1013）の各々へ固定的に関連付けられた物理インタフェースまたは固定論理インタフェースである。PC等ユーザ端末が送受信する、ユーザデータを構成するIPパケットは、PC等ユーザ端末からアクセスルータ500までの間はPPPにカプセル化されて送受信されるが、インタフェース1041～1043上ではピュア・IPパケットとして送受信される。

VR1～3（1011～1013）の各々はあたかも独立のLNS装置であるかのように動作する。例えばVR1（1011）は、VR0（1010）からマッピングされたL2TPトンネルを確立する際のセットアップ情報、ユーザ認証の際に連携するAAAサーバ1061の情報、IPアドレス情報、経路制御情報、サービス品質制御情報等を、VR2（1012）、VR3（1013）の存在を意識することなく独立に設定することができる。このように、VR1～3（1011～1013）を、それぞれISP1～3と接続するための独立した仮想LNS装置として運用することにより、

第４実施例と同様に、アクセスルータ500の単一の物理筐体によって複数のISPとの接続が可能となる。

VR1～3（1011～1013）は、自身にマッピングされたL2TPトンネルや、各々をISP1～3の網（1051～1053）と接続するインタフェース1041～1043に関わる管理権限等を有するが、アクセスルータ500の装置全体に関わる管理権限は有さない。このことは、アクセス回線事業者またはL2TP転送網1030を所有する事業者がISP事業者1～3にVR1～3（1011～1013）の各々を仮想的なLNS装置としてホールセール（卸売り、管理権限委譲）するのに適している。アクセス回線事業者またはL2TP転送網1030を所有する事業者はVR0（1010）の管理権限、すなわちアクセスルータ500の装置全体の管理権限を有するので、ISP事業者1～3に管理権限を委譲したVR1～3（1011～1013）の運用状況を監視することができ、また必要に応じて権限委譲のレベルを設定したり、スーパバイザ権限により強制的なコマンド発行等も可能である。また、L2TP転送網1030側に接続するVR0（1010）と、ISP事業者1～3の網（1051～1053）に接続するVR1～3（1011～1013）を分離することにより、L2TP転送網のIPアドレス空間はアクセス回線事業者またはL2TP転送網1030を所有する事業者が行い、ユーザ認証を含むPPPセッションの運用管理は各々のISPが行うというように、管理権限を明確に分離した事業者間の分業形態が可能となる。また、L2TPトンネルおよびこれに多重されたL2TPセッションを終端するのはVR1～3（1011～1013）であるので、L2TPトンネルおよびこれに多重されたL2TPセッションの運用管理を各々のISPに委譲することもできる。セキュリティ等の観点からL2TP関連の運用管理をISPから隠蔽したい場合には、VR0（1011）の有するスーパバイザ権限によりVR1～3（1011～1013）におけるL2TP関連の設定コマンドへのアクセスを制限することができる。

図１に示した従来技術を用いた場合には、LNS131とISP1網142の接続のためにGW141が必要であった。一方、本実施例ではVR0（1010）がL2TP転送網1030側のIPアドレス空間を終端する仮想的なエッジノードの役割を果たし、VR1～3（1011～1013）はそれぞれISP1～3の網（1051～1053）側のIPアドレス空間を終端する仮想的なエッジノードの役割を果たす。すなわち、VR1～3（1011～1013）自体がゲートウェイルータの役割を果たすことが可能である。例えば経路制御を自動化するためのOSPFやBGPといったルーティングプロトコルはVR0～3（1010～1013）の各々で独立に動作させることが可能であり、その際VR0（1010）はL2TP転送網1030側の経路制御ドメインのエッジを構成し、VR1～3（1011～1013）はそれぞれISP1～3の網（1051～1053）側の経路制御ドメインのエッジを構成することができる。また、VR0（1010）とVR1～3（1011～1013）の各々と

の間の内部的なデータ送受はL2TPレイヤのマッピングによって行われるため、VR0（1010）とVR1～3（1011～1013）の各々との間ではIPレイヤの相互作用がない。従って、従来技術や第４実施例を用いた場合のような、L2TP転送網1030とISP1～3の網（1051～1053）との間でピュア・IPパケットが透過するような状況は本来的に起こり得ず、アクセス回線事業者または中継事業者とISP1～3との間では強固なセキュリティが確保される。また、PC等ユーザ端末からはL2TP転送網1030の存在は完全に隠蔽され、PC等ユーザ端末とL2TP転送網1030内のノード等との間のIP通信は本来的に起こり得ないので、従来技術や第４実施例を用いた場合のような、VR1～3（1011～1013）がPPPセッション上で受信したIPパケットをISP1～3の網（1051～1053）へ強制的にルーティングするためのポリシールーティングの設定を行う必要もない。このように、VR1～3（1011～1013）をゲートウェイ機能を有する仮想的なLNS装置としてホールセールすることによって、従来ならば別途必要であったゲートウェイルータが本実施例では不要である。ISP1～3は、インタフェース1041～1043を自身の網1151～1153に収容するために高価なゲートウェイルータを設置する必要はなく、安価なレイヤ2スイッチまたはレイヤ3スイッチを用いて収容することができる。

L2TP転送網用インタフェース1031～1033は、各々独立した物理インタフェースであっても良いし、単一の物理インタフェースに多重された固定論理インタフェースであっても良い。固定論理インタフェースの例としては、ATM PVC、IEEE802.1Q TAG VLAN、MPLSラベルパス等が挙げられる。また、アクセスルータ500がLNS装置として最低限の役割を果たすためには、L2TP転送網用インタフェースは少なくとも1つあれば良い。本実施例のように複数のL2TP転送網用インタフェースを用いる場合のメリットとしては、L2TP転送網1030とVR0（1010）との間の通信における、帯域の増強、経路の冗長化・分散化等が挙げられる。これは図１に示した従来技術を用いた場合と同様である。

L2TP転送網用インタフェース1021～1023と、L2TPトンネル1024～1026との間には、各々特定の関連付けは存在しない。例えばL2TPトンネル1024を構成するL2TPパケットは通常のIPパケットとして送受信されるので、送信時・受信時共に、各々のルータ装置の経路情報テーブルに従ってフォワーディングされる。従って、前記L2TPパケットがL2TP転送網用インタフェース1021～1023のいずれを用いて送受信されるかは固定的に決まっておらず、L2TP転送網1030のネットワーク構成の変化やL2TP転送網用インタフェースのいずれかに発生した障害等に起因して経路情報が変化した場合には、変更後の経路情報テーブルに従ってフォワーディングされる。従って、例えばそれまで用いていたL2TP転送網用インタフェース1021が何らかの原因により送受信できなくなっ

た場合でも、L2TP転送網用インタフェース1022、1023のいずれかを用いた経路に切り替わればL2TPパケットは継続的に送受信可能である。これは図１に示した従来技術を用いた場合と同様である。

図１８は、本実施例における接続シーケンスの一例である。これらのシーケンスの実行制御は、図２に示したアクセスルータ構成例においてはシーケンス制御部573が行う。仮想ルータ管理部571や仮想ルータ構成テーブル572と連携することにより、運用設定がLAC型/LNS型のいずれであるか、マッピング設定が固定マッピング/L2TPマッピング/PPPマッピングのいずれであるかを識別し、図１８のシーケンスのいずれかを実行する。

以上、本実施例に記載のLNSにより、第４実施例に記載した５つの効果の他、次のような効果が得られる。

第４実施例と異なり、ISP網との接続のために別途ゲートウェイルータが必要ない。

また、ISP網側の仮想ルータを、該ISP自身のゲートウェイルータとしてホールセールし、ルーティングドメインやセキュリティドメインを自由に設計させることが可能となる。

【第６実施例】

図１９は、本発明の第６のマッピング方式（LNS型・PPPマッピング方式）に関する実施形態の一例であり、アクセスルータおよびネットワークの構成を示す。

VR0（1110）は、第４実施例の場合と同様にアクセスルータ500の装置全体に関わる管理権限を有し、また第４実施例の場合と同様にL2TP転送網用インタフェース1121～1123を管理する役割を担う。L2TPトンネル1124～1126およびそれらに多重されたL2TPセッションは、L2TP転送網用インタフェース1121～1123のいずれかを用いて受信され、VR0（1110）において完全に終端される。すなわち、L2TPトンネル1124～1126を構成するL2TPパケットはVR0（1110）においてL2TPヘッダを外され、PPPフレームが取り出される。L2TPトンネル1124～1126より取り出されたこれらのPPPセッションは、各々VR1～3（1111～1113）へマッピングされ、該マッピング先のVRにおいて終端される。マッピングを行うために基づく情報としては、第３実施例の場合と同様、PPPセッション単位で異なる値を持ち得る任意の属性情報であって構わない。そのような属性情報の例として、セッション確立時にLACがICCNメッセージにより通知する各種情報（ユーザ識別文字列中のISP識別情報、LCPフェーズにおけるネゴシエーション結果の各種パラメータ値、伝送速度、Private Group ID値等）、L2TPセッション接続要求を着信した時点におけるVR1～3（1111～1113）のリソース占有情報、AAAサーバ1161～1163あるいは他

のネットワーク監視サーバから取得したISP1～3の網1151～1153各々の輻輳情報、等が挙げられる。

図20Aおよび図20Bには、本実施例で用いられる論理Ｉ/Ｆテーブル545と経路情報テーブル546の内容を示す。論理Ｉ/Ｆテーブルは、仮想ルータ識別子を格納する仮想ルータフィールド2501、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2502、受信パケットのプロトコルの種別を示す識別子を格納するプロトコルフィールド2503、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2504、該当する物理Ｉ/Ｆおよび論理Ｉ/Ｆが、パケットの送信送信（transmit）を行なう通信Ｉ/Ｆかパケットを着信（receive）する通信Ｉ/Ｆかの別を示す値が格納されるDirectionフィールド2505、当該パケットに対して実行するべき処理内容を示す情報が格納されるアクションフィールド2506および仮想ルータフィールド2507からなる。物理Ｉ/Ｆ識別子としては、例えば、ATM_11やEther_12等、受信パケットが属するセッションで使用されているプロトコルに適当な数字を加えた識別子や、あるいは単純にポート番号等を使用する。

経路情報テーブル546は、仮想ルータ識別子を格納する仮想ルータフィールド2511、受信パケットの宛先IPアドレスが格納される宛先IPアドレスフィールド2512、アドレスマスクが格納されるアドレスマスクフィールド2513、処理しようとするパケットが自宛パケットかそうでないかを示す識別子が格納される自宛フィールド2514、nexthopノードのアドレスが格納されるNextHopアドレスフィールド2515、物理Ｉ/Ｆ識別子を格納する物理Ｉ/Ｆフィールド2516、論理Ｉ/Ｆ識別子を格納する論理Ｉ/Ｆフィールド2517からなる。

以下に、図20Aに示す論理Ｉ/Ｆテーブルおよび図20Bに示す経路情報テーブルを用いたマッピング方法について説明する。各フィールドには、仮想ルータ識別子フィールド以外は、第４実施例に示した値と同じ値が格納されている。上り方向の検索時には、2521～2528行の順番でエントリが検索される。2521～2524行の検索時には、L2TPパケット（＝IPパケット）の受信はVR_0で行われ、L2TPを終端（デカプセル化）した後に、VR_1へマッピングされる。2525～2532行の検索時には VR_1でPPPが終端（デカプセル化）され、VR_1の経路情報に基づきISP網へルーティングされる。下り方向の検索時には、2531～2538の順番でエントリが検索される。2531～2533行の検索時には PC等ユーザ端末宛のIPパケットはVR_1で受信され、PPPにカプセル化された後にVR_0へマッピングされる。2534～2538行の検索時には PPPがさらにL2TPへカプセル化され、VR_0の経路情報に基づきL2TPパケット（＝IPパケット）がLAC装置宛にルーティングされる。

PPPセッション単位で動的に仮想ルータへのマッピングを行う本実施例に拠れば、従

来実現されることのなかった多様な形態でのネットワーク設計やサービス提供が可能となる。一例として、ユーザ識別文字列中のISP識別情報（例："isp1.co.jp"）に基づいて前記マッピングを行う場合、ISP1～3に共通のアクセスメニューを利用するユーザのセッションを、どのISPへのセッションであるかに関係なく共通のL2TPトンネルへ多重化することが可能となる。例えばL2TPトンネル1124には1.5MbpsのADSLユーザのセッションを、L2TPトンネル1125には8MbpsのADSLユーザのセッションを、L2TPトンネル1126には100MbpsのFTTHユーザのセッションを多重化することにより、L2TP転送網1130における経路制御や帯域制御を、サービスメニュー毎に木目細かく設計することが可能になる。別の例として、ISP1～3の網1151～1153各々の輻輳情報に基づいて前記マッピングを行う場合、例えばISP1～3が一つの仮想的なプロバイダを形成し、ユーザからの接続要求時に最も輻輳状況の小さいISPへ接続するといった新たなサービス形態が可能となる。

VR0（1110）はアクセス回線事業者またはL2TP転送網1130を所有する事業者の管理専用の仮想ルータであると同時に、L2TP転送網用インタフェース1121～1123を一括して管理し、全てのL2TPトンネルおよびこれらに多重されたL2TPセッションを終端し、取り出したPPPセッションのVR1～3（1111～1113）へのマッピングを管理するという意味で言わば「代表VR」であり、L2TPを終端すると言う意味で従来のLNS型アクセスルータのイメージに対応する。図１９中、VR0（1110）の左下部分に"V-LNS"（Virtual-LNS）と表記しているのは本イメージを意味したものである。一方、PPPセッションのマッピング先であるVR1～3（1111～1113）は、AAAサーバ1161～1163と連携してユーザ認証を行い、PC等ユーザ端末との間でPPPセッションを確立するという意味で従来のBAS（Broadband Access Server）型アクセスルータのイメージに対応する。また、図１９中、VR1～3（1111～1113）の右下部分に"V-BAS"（Virtual-BAS）と表記しているのは本イメージを意味したものである。

なお本実施例では、インタフェース1120は第４実施例におけるインタフェース920と同様の管理専用インタフェースと想定しているが、リモートログインを実現するためにL2TP転送網1130に接続するのであれば、必ずしも管理専用としなくても良い。インタフェース1121～1123と同様に、L2TPパケットの送受信にも同時に用いることも可能である。セキュリティ等への考慮から、特定のインタフェースに限定してリモートログインを許容したい場合等には、本実施例のように管理専用のインタフェースとL2TPパケットの送受信用のインタフェースを分けるのが良い。

VR1～3（1111～1113）とISP1～3の網（1151～1153）とを接続するインタフェース1141

～1143は、VR0（1110）の管理権限によってVR1～3（1111～1113）の各々へ固定的に関連付けられた物理インタフェースまたは固定論理インタフェースである。PC等ユーザ端末が送受信する、ユーザデータを構成するIPパケットは、PC等ユーザ端末からアクセスルータ500までの間はPPPにカプセル化されて送受信されるが、インタフェース1141～1143上ではピュア・IPパケットとして送受信される。

これらの固定論理インタフェースは、コマンド設定等によって明示的にマッピング設定が行われるものであって、装置の運用中に自動的に生成または削除されたり、異なるマッピング設定に切り替わったりすることはない。具体例として、ATM PVC、IEEE802.1Q TAG VLAN、MPLSラベルパス、また、該物理インタフェース上で複数のプロトコルを多重化する場合の、各々のプロトコルに対応する設定単位であるサブインタフェース、等が挙げられる。

VR1～3（1111～1113）の各々はあたかも独立のBAS装置であるかのように動作する。例えばVR1（1111）は、VR0（1110）からマッピングされたPPPセッションを確立する際に連携するAAAサーバ1161の情報、IPアドレス情報、経路制御情報、サービス品質制御情報等を、VR2（1112）、VR3（1113）の存在を意識することなく独立に設定することができる。このように、VR1～3（1111～1113）を、それぞれISP1～3と接続するための独立した仮想BAS装置として運用することにより、第４実施例や５と同様に、アクセスルータ500の単一の物理筐体によって複数のISPとの接続が可能となる。

VR1～3（1111～1113）は、自身にマッピングされたPPPセッションや、各々をISP1～3の網（1151～1153）と接続するインタフェース1141～1143に関わる管理権限等を有するが、アクセスルータ500の装置全体に関わる管理権限は有さない。このことは、アクセス回線事業者またはL2TP転送網1130を所有する事業者がISP事業者1～3にVR1～3（1111～1113）の各々を仮想的なBAS装置としてホールセール（卸売り、管理権限委譲）するのに適している。アクセス回線事業者またはL2TP転送網1130を所有する事業者はVR0（1110）の管理権限、すなわちアクセスルータ500の装置全体の管理権限を有するので、ISP事業者1～3に管理権限を委譲したVR1～3（1111～1113）の運用状況を監視することができ、また必要に応じて権限委譲のレベルを設定したり、スーパバイザ権限により強制的なコマンド発行等も可能である。また、L2TP転送網1130側に接続するVR0（1110）と、ISP事業者1～3の網（1151～1153）に接続するVR1～3（1111～1113）を分離することにより、L2TPトンネルおよびこれに多重されたL2TPセッションの運用管理はアクセス回線事業者またはL2TP転送網1130を所有する事業者が行い、ユーザ認証を含むPPPセッションの運用管理は各々のISPが行うというように、管理権限を明確に分

離した事業者間の分業形態が可能となる。

図１に示した従来技術を用いた場合には、LNS131とISP1網142の接続のためにGW141が必要であった。一方、本実施例では第４実施例の場合と同様に、VR0（1110）がL2TP転送網1130側のIPアドレス空間を終端する仮想的なエッジノードの役割を果たし、VR1～3（1111～1113）はそれぞれISP1～3の網（1151～1153）側のIPアドレス空間を終端する仮想的なエッジノードの役割を果たす。すなわち、VR1～3（1111～1113）自体がゲートウェイルータの役割を果たすことが可能である。例えば経路制御を自動化するためのOSPFやBGPといったルーティングプロトコルはVR0～3（1110～1113）の各々で独立に動作させることが可能であり、その際VR0（1110）はL2TP転送網1130側の経路制御ドメインのエッジを構成し、VR1～3(1111～1113)はそれぞれISP1～3の網(1151～1153)側の経路制御ドメインのエッジを構成することができる。また、VR0（1110）とVR1～3（1111～1113）の各々との間の内部的なデータ送受はPPPレイヤのマッピングによって行われるため、VR0（1110）とVR1～3（1111～1113）の各々との間ではIPレイヤの相互作用がない。従って、従来技術や第４実施例を用いた場合のような、L2TP転送網1130とISP1～3の網（1151～1153）との間でピュア・IPパケットが透過するような状況は本来的に起こり得ず、アクセス回線事業者または中継事業者とISP1～3との間では強固なセキュリティが確保される。また、PC等ユーザ端末からはL2TP転送網1130の存在は完全に隠蔽され、PC等ユーザ端末とL2TP転送網1130内のノード等との間のIP通信は本来的に起こり得ないので、従来技術や第４実施例を用いた場合のような、VR1～3（1111～1113）がPPPセッション上で受信したIPパケットをISP1～3の網（1151～1153）へ強制的にルーティングするためのポリシールーティングの設定を行う必要もない。このように、VR1～3（1111～1113）をゲートウェイ機能を有する仮想的なBAS装置としてホールセールすることによって、従来ならば別途必要であったゲートウェイルータが本実施例では不要である。ISP1～3は、インタフェース1141～1143を自身の網1151～1153に収容するために高価なゲートウェイルータを設置する必要はなく、安価なレイヤ2スイッチまたはレイヤ3スイッチを用いて収容することができる。

L2TP転送網用インタフェース1131～1133は、各々独立した物理インタフェースであっても良いし、単一の物理インタフェースに多重された固定論理インタフェースであっても良い。固定論理インタフェースの例としては、ATM PVC、IEEE802.1Q TAG VLAN、MPLSラベルパス等が挙げられる。また、アクセスルータ500がLNS装置として最低限の役割を果たすためには、L2TP転送網用インタフェースは少なくとも1つあれば良い。本実施例のように複数のL2TP転送網用インタフェースを用いる場合のメリットとしては、

L2TP転送網1130とVR0（1110）との間の通信における、帯域の増強、経路の冗長化・分散化等が挙げられる。これは図１に示した従来技術を用いた場合と同様である。

L2TP転送網用インタフェース1121～1123と、L2TPトンネル1124～1126との間には、各々特定の関連付けは存在しない。例えばL2TPトンネル1124を構成するL2TPパケットは通常のIPパケットとして送受信されるので、送信時・受信時共に、各々のルータ装置の経路情報テーブルに従ってフォワーディングされる。従って、前記L2TPパケットがL2TP転送網用インタフェース1121～1123のいずれを用いて送受信されるかは固定的に決まっておらず、L2TP転送網1130のネットワーク構成の変化やL2TP転送網用インタフェースのいずれかに発生した障害等に起因して経路情報が変化した場合には、変更後の経路情報テーブルに従ってフォワーディングされる。従って、例えばそれまで用いていたL2TP転送網用インタフェース1121が何らかの原因により送受信できなくなった場合でも、L2TP転送網用インタフェース1122、1123のいずれかを用いた経路に切り替わればL2TPパケットは継続的に送受信可能である。これは図１に示した従来技術を用いた場合と同様である。

LAC装置との間でL2TPトンネル1124～1126を確立する際には、トンネルセットアップ情報はVR0(1110)において設定する。あるいは、トンネルセットアップ情報をVR0(1110)自体には設定せず、AAAサーバ1131に問い合わせて取得することも可能である。そのようなトンネルセットアップ情報の例として、トンネルID、トンネルパスワード、LAC装置識別文字列、LNS装置識別文字列、LAC側トンネル終端IPアドレス、LNS側トンネル終端IPアドレス等が挙げられる。またAAAサーバ1131は、トンネルセットアップ情報を管理する以外にも、L2TPトンネルおよびこれに多重されたL2TPセッションのアカウンティング情報を収集・蓄積する外部データベースサーバとしても使用できる。そのようなアカウンティング情報の例として、トンネルID、セッションID、ユーザ情報文字列、トンネルまたはセッションの継続時間、送受信オクテット数、送受信パケット数等が挙げられる。このような外部サーバを用いてトンネルセットアップ情報やアカウンティング情報を管理することにより、大規模なL2TPネットワークにおける多数のLAC装置やLNS装置を効率的に運用管理することが可能である。

従来技術を用いたLNS装置では、認証用途のAAAサーバとアカウンティング用途のAAAサーバを独立に設定することは可能であった。しかし、本実施例のようにL2TPプロトコルの管理（AAAサーバ1131）とPPPプロトコルの管理（AAAサーバ1161～1163）で異なるAAAサーバを設定することはできなかった。従来、LNS装置におけるAAAサーバの主要用途はISPにおけるユーザ認証およびPPPセッションのアカウンティングであったため、

図１におけるAAAサーバ143のように、ISP網内に設置する場合が多かった。しかしL2TP転送網が大規模になれば、前述のようにL2TPプロトコルの管理もAAAサーバで行うことへの需要が高まる。ところがL2TPプロトコルはアクセス回線事業者またはL2TP転送網1130を所有する事業者の管理下にあるため、その管理をISP網側に設置したAAAサーバに委ねるのは事業形態の観点およびセキュリティの観点から望ましくない。本実施例は、従来のLNS装置におけるこのような制約を、L2TPプロトコルを終端するVR0（1110）とPPPプロトコルを終端するVR1～3（1111～1113）を分離することによって、L2TPプロトコルを管理するAAAサーバ1131はL2TP転送網1130内に設置し、ユーザ認証を含むPPPプロトコルを管理するAAAサーバ1161～1163はISP1～3の網（1151～1153）内に設置するというように自然な形で解決している。必要であれば、AAAサーバ1131を、L2TPトンネルセットアップの用途とL2TPトンネルおよびセッションのアカウンティングの用途で別々のサーバを設定することも可能である。

以上のように、本マッピング方式に拠れば（LNSにおける課題１～６）の各々を解決することができる。

図２１は、本実施例に示した（LNS型・PPPマッピング方式）における接続シーケンスの一例である。アクセスルータ500がLAC1711との間で、図１９に示したL2TPトンネル1124および本トンネルに多重されたL2TPセッション1127を確立するまでの正常シーケンスを示す。なお、以降の説明においては、図２に示したアクセスルータ構成例に特化した説明ではなく、仮想ルータ間の論理的な連携方法の説明を行っている。図２に示したアクセスルータ構成例においては、実行主体はシーケンス制御部573であるので、例えば以降の説明における「VR0がある動作を実行する」という表現は、「VR0を示す仮想ルータ識別子のコンテキストにおいて、シーケンス制御部573がある動作を実行する」と言い換えることができる。

LAC1711とVR0（1110）の間のシーケンス1721～1724、1741～1744は、RFC2661の規定するL2TPプロトコルの通常の接続シーケンスである。また、VR0（1110）とAAAサーバ1131の間のシーケンス1731～1734、VR1（1111）とAAAサーバ1161の間のシーケンス1761、1762の各々は、例えばRADIUSプロトコルの規定する一往復の問い合わせシーケンスが使用可能である。このように、アクセスルータ500は内部的には仮想ルータ間の連携により全体のシーケンスが制御されるが、個々の外部シーケンスは従来の標準技術に変更を加えるものではない。

L2TPトンネル1124の確立シーケンス1720は、LAC1711とVR0（1110）の間のシーケンス1721～1724と、VR0（1110）とAAAサーバ1131の間のシーケンス1731～1734によって

構成される。手順1731は、AAAサーバ1131が保持するトンネルセットアップ情報の問い合わせである。手順1732により受信した問合わせ結果に基づき、手順1722におけるパラメータ指定を行う。なお、VRO（1110）自身がトンネルセットアップ情報をローカルに保持している場合には、本問い合わせ手順1731、1732は不要である。

手順1733は、AAAサーバ1131へのトンネル認証の問い合わせである。手順1734により受信した認証結果がOKであるならば、手順1724によりLAC1711へ接続完了を通知する。なお、VRO（1110）自身が認証パスワードをローカルに保持している場合やトンネル認証を行わない場合には、本問い合わせ手順1733、1734は不要である。

L2TPセッション1127の確立シーケンス1740は、LAC1711とVRO（1110）の間のシーケンス1741～1744と、VR1（1111）とAAAサーバ1161の間のシーケンス1761～1764によって構成される。また、これら外部シーケンスに付随し、VRO（1110）とVR1（1111）との間の連携手順1751～1753が実行される。

LAC1711が手順1743によりVRO(1110)へセッション属性情報を通知すると、VRO(1110)は手順1751により、あらかじめ定義してあるマッピング規則を前記セッション属性情報またはその他の属性情報に対して適用し、L2TPセッション1127のマッピング先をVR1（1111）に決定する。マッピング規則が基づくことのできる属性情報の詳細は、先に示した通りである。

マッピング先がVR1（1111）に決定すると、手順1752により、VRO（1110）がVR1（1111）に対してユーザ認証の実行を依頼する。VR1（1111）は手順1761によりAAAサーバ認証1161へユーザ認証を問い合わせる。なお、VR1（1111）自身が認証データベースをローカルに保持している場合や認証自体を行わない場合には、本問い合わせ手順1761、1762は不要である。手順1762により認証OKが通知されると、手順1753により、VR1（1111）がVRO（1110）に対して認証完了を通知し、同時にVRO（1110）ではL2TPセッション1127用の内部リソースがセットアップされ、VR1（1111）ではこれに対応するPPPセッションの内部リソースがセットアップされ、両者が連結される。VRO（1110）が手順1744によりLAC1711へセッション確立通知を送信することによって、L2TPセッション1127の確立が完了する。この後引き続いてPPPのIPCPフェーズ1770に移行するが、これはPC等ユーザ端末1712とVR1（1011）の間で行われる。

なお、図１７には記載していないが、VRO（1110）とAAAサーバ1131の間では、L2TPトンネルとそれらに多重化されたL2TPセッションに関する統計情報を収集するためのアカウンティングシーケンスを実行することができる。本シーケンスは、L2TPトンネルまたはL2TPセッションの接続または切断が発生した時点での実行や、例えば10分に

一度の定期的な実行を行うことができる。同様に、VR1（1111）とAAAサーバ1161の間では、VR1（1111）にマッピングされたPPPセッションに関する統計情報を収集するためのアカウンティングシーケンスを実行することができる。本シーケンスは、PPPセッションの接続または切断が発生した時点での実行や、例えば10分に一度の定期的な実行を行うことができる。

以上、本実施例に記載のLNSにより、第４実施例に記載した５つの効果の他に、特定のL2TPトンネル内に、ISPによらずに自由にPPPセッションを多重することができるという効果が得られる。従来のLNS装置は、別々のISPへ向かうPPPセッションを多重したL2TPトンネルから個々のPPPセッションを別々に取り出して終端することができず、特定のL2TPトンネルへは特定のISP向けのPPPセッションしか多重できなかった。従って、L2TP転送網内での多重化の方法が限定されていた。

上記記載は実施例についてなされたが、本発明はそれに限らず、本発明の精神と添付のクレームの範囲内で種々の変更および修正をすることができることは当業者に明らかである。

What is claimed is:

１、LNS機能ないしLAC機能を備えた仮想アクセスルータは、

パケットを送受信する複数の通信Ｉ/Ｆと、

該通信Ｉ/Ｆと対応づけられ、ユーザ端末との間でパケットを送受信する複数の第１の論理インタフェースと、

前記通信Ｉ/Ｆと対応づけられ、バックボーンネットワークとの間でパケットを送受信する複数の第２の論理インタフェースと、

仮想ルータが各々管理する経路情報を格納する経路情報テーブルと、

仮想ルータの１を前記第１のインタフェースおよび第２のインタフェースの１つに関連付ける手段とを有し、

前記第１のインタフェースより受信したパケットを、前記第１の論理インタフェースが関連付けられた仮想ルータに対応した経路情報テーブルに基づいて、前記仮想ルータに関連付けられた前記第２の論理インタフェースのいずれかに転送する。

２、請求項１に記載の仮想アクセスルータは、

L2TP LAC機能を有し、

前記複数の通信Ｉ/Ｆのいずれかに割り当てられたPPPフレームを送受信するための通信Ｉ/ＦないしPPPセッションに対応する論理インタフェースを前記第１の論理インタフェースとし、

L2TPパケットを送受信するためのインタフェースを前記第２のインタフェースとし、

前記仮想ルータの各々において前記L2TP LAC機能が動作する。

３、請求項１に記載の仮想アクセスルータは、

L2TP LAC機能を有し、

複数のL2TPトンネルを終端する機能を有し、

該複数のL2TPトンネルの１に対応する論理インタフェースを前記第１のインタフェースとし、

L2TPパケットを送受信するためのインタフェースを前記第２のインタフェースとし、

前記L2TP LAC機能によりユーザ端末からのPPPセッションを前記第１のインタフェースに関連付ける。

４、請求項１に記載の仮想アクセスルータは、

L2TP LNS機能を有し、

前記複数の通信Ｉ/Ｆに割り当てられたL2TPパケットを送受信するための通信Ｉ/Ｆないし L2TPトンネルに対応する論理インタフェースを前記第１の論理インタフェースとし、

バックボーンネットワークとの間でパケットを送受信するためのインタフェースを前記第２のインタフェースとし、

前記仮想ルータの各々において前記L2TP LNS機能が動作する。

５、請求項１に記載の仮想アクセスルータは、

L2TP LNS機能を有し、

受信したPPPセッションに対応する論理インタフェースを前記第１の論理インタフェースとし、

バックボーンネットワークとの間でIPパケットを送受信するためのインタフェースを前記第２の論理インタフェースとし、

前記L2TP LNS機能が、L2TPトンネルに多重されたPPPセッションを前記第１の論理インタフェースに関連付ける。

６、請求項１に記載の仮想アクセスルータは、

前記関連づける手段を、仮想ルータの１つにより実現する。

７、請求項１に記載の仮想アクセスルータは、

前記通信Ｉ/Ｆのいずれかで受信された制御用の管理コマンドにより、前記第１の論理インタフェースと前記仮想ルータとの対応関係、および前記第２の論理インタフェースと前記仮想ルータとの対応関係が変更可能である。

８、仮想アクセスルータは、

外部の通信回線に接続するための複数の通信Ｉ/Ｆと、

該端子を介して送受信されるパケットに対して所定の処理を行なうためのプロセッサと、

受信パケットに対して所定の処理を行なうための参照情報が格納されるメモリとを有し、

該メモリには、

受信パケットの物理インタフェース識別子ないし論理インタフェース識別子と、該識別子に対応する仮想ルータ識別子との関係を保持するインタフェーステーブルと、

前記仮想ルータ識別子に対応する仮想ルータで処理すべき経路情報を保持する経路情報テーブルとが格納され、

前記プロセッサは、

受信パケットに対し、前記インタフェーステーブルを参照して、該受信パケットを処理すべき仮想ルータの識別子を特定し、

前記経路情報テーブルから、前記仮想ルータ識別子に対応する仮想ルータが管理する経路情報を読み出して、前記受信パケットの転送処理を行なう。

９、請求項８に記載の仮想アクセスルータにおいて、

前記インタフェーステーブルと前記経路情報テーブルとが、互いに異なるメモリに格納される。

１０、請求項８に記載の仮想アクセスルータにおいて、

前記論理インタフェース識別子として、L2TPトンネルの識別子、PPPセッションの識別子ないし外部通信回線を介して接続されるインタネットサービスプロバイダの識別子を用いる。

１１、請求項８に記載の仮想アクセスルータにおいて、

前記物理インタフェース識別子として、前記複数の通信Ｉ/Ｆのポート番号を用いる。

１２、請求項８に記載の仮想アクセスルータにおいて、

LAC機能またはLNS機能を備える。

１３、　請求項１２に記載の仮想アクセスルータにおいて、

前記メモリには、受信パケットをL2TPトンネルを生成するシーケンスとL2TPトンネルを終端するシーケンスとが格納され、

前記プロセッサがいずれのシーケンスを読み出して実行することにより、前記LAC機能およびLNS機能を実現する。

１４、請求項１２に記載の仮想アクセスルータは、
前記LAC機能ないしLNS機能を切替える手段を備えた。

１５、請求項１３に記載の仮想アクセスルータにおいて、
前記プロセッサがいずれのシーケンスを読み出すか設定する手段を備え、
該設定手段により、前記LAC機能とLNS機能を切替える。

１６、　請求項８に記載の仮想アクセスルータは、
前記通信Ｉ/Ｆで受信した管理用制御コマンドの内容を分析するためのプログラムを格納したプログラムメモリを備え、
前記プロセッサは、前記管理用制御コマンドを実行することにより、契約で認められた制御コマンド発信元に対しては全ての仮想ルータに対応するインタフェーステーブルの設定変更を認める。

１７、請求項１６に記載の仮想アクセスルータにおいて、
前記プロセッサは、前記管理用制御コマンドを実行することにより、特定の制御コマンド発信元に対しては、特定の仮想ルータに対応するインタフェーステーブルの設定変更のみ認める。

１８、請求項１７に記載の仮想アクセスルータを使用した事業形態であって、
前記仮想アクセスルータを所有または管理する通信事業者が、別の通信事業者のネットワークへ接続するインタフェースを特定の仮想ルータに関連付け、該仮想ルータに対応する管理用制御コマンドの使用権限を前記通信事業者に委譲する。

Abstract of the disclosure

LAC装置またはLNS装置を構成するアクセスルータに仮想ルータ機能を持たせ、物理インタフェースまたは固定論理インタフェースの単位、L2TPトンネルの単位、PPPセッションの単位のいずれかによって仮想ルータへの関連付けを行う。それにより、1台のLAC装置またはLNS装置を、異なる事業者の管理する複数のL2TP転送網、または複数のISP網と接続させる。